DRAFT-PWS 160054

25 October 2016

PERFORMANCE WORK STATEMENT (PWS)

FOR

SOFTWARE ENGINEERING, ANALYSIS, CONTENT DEVELOPMENT, LOGISTICS, AND LIFE CYCLE SUPPORT SERVICES FOR AUTHORING INSTRUCTIONAL MATERIALS (AIM)

CROSS WARFARE SUPPORT BRANCH

NAVAL AIR WARFARE CENTER TRAINING SYSTEMS DIVISION

ORLANDO, FL 32826

DISTRIBUTION STATEMENT C - Distribution authorized to U.S. Government agencies and their contractors (Administrative or Operational Use: To protect technical or operational data or information from automatic dissemination under the International Exchange Program or by other means.) (1 Mar 2014).

WARNING - This document contains technical data whose export is restricted by the Arms Export Control Act (Title 22, U.S.C., Sec 2751, et seq.) or the Export Administration Act of 1979 (Title 50, U.S.C., App. 2401 et seq.), as amended. Violations of these export laws are subject to severe criminal penalties. Disseminate in accordance with provisions of DoD Directive 5230.25.

DESTRUCTION NOTICE - For unclassified, limited distribution documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

This page left intentionally blank

Table of Contents

Table of Contents

Table of Contents

APPENDICES

Performance Work Statement (PWS)

For

Software Engineering, Analysis, Content Development, Logistics, and Life Cycle Support Services for Authoring Instructional Materials (AIM)

1. SCOPE

This PWS identifies and defines the requirements for the Contractor to provide software engineering, analysis, content development, logistics, and life cycle support services for the Authoring Instructional Materials (AIM) program. The Naval Air Warfare Center Training Systems Division (NAWCTSD) is the System Support Office (SSO) for AIM. The AIM SSO provides overall programmatic and technical management as well as end-user support to the AIM user community.

1.1 AIM Background

AIM is a set of software tools designed to improve, streamline, and automate certain aspects of the development and maintenance of Navy training materials. The Navy uses three different approaches for the development of training materials: Personnel Performance Profile (PPP), Task-Based, and Competency/Skills-Based. AIM I supports the PPP approach to training material development, AIM II supports the Task-Based approach, and AIM Content Planning Module (CPM)/Learning Object (LO) Module supports a Competency/Skills-Based or Integrated Learning Environment (ILE) approach. These tools allow for more efficiency and responsiveness in the production and life cycle maintenance of training materials to Navy training activities and to other organizations external to the Navy. AIM also optimizes the process of instructional development and standardizes the training materials by automating the format and standards promulgated in various military and commercial training design/ development standards. AIM I, II, and CPM/LO Module all operate in the Microsoft MS Windows environment to provide a graphical user interface.

AIM access is currently provided from a centralized government hosted environment where users can access the AIM software and database from geographically dispersed locations. This AIM Central Site effort provides AIM software access and related data to an increasingly wider Navy audience while facilitating data integrity and concurrency. For those users who are not able to access the centralized environment, standalone instances of the AIM software are still in use. CPM is web-based and current plans for the AIM project includes the eventual suspension of the AIM I &II applications, and the merging of the LO Module with CPM for a fully web-based AIM application.

A major driver of future potential AIM functionality is the Navy's Ready Relevant Learning (RRL) effort. This strategic initiative, with a focus on RRL is focused on delivering training in a modular construct through immersive and interactive learning capabilities, providing just in time training when a Sailor needs it.

AIM requirements will continue to evolve as the Navy's RRL initiative and other Competency/Skills-Based approaches mature. These requirements are defined by the Navy's AIM governance organizations (Configuration Control Board (CCB)), Executive Steering Committee (ESC), and Functional Requirements Board (FRB).

2. GOVERNMENT STANDARDS

The following government standards apply:

IEEE/EIA 12207-2008	-	Information Technology – Software Life-Cycle Processes
MIL-PRF-29612B	-	Training Data Products, August 2001
DODI 8510.01	-	Risk Management Framework for DoD Technology
DoD 5220.22-M	-	National Industrial Security Program Operating Manual (NISPOM), 28 February 2006, Change 2, 18 May 2016.
SECNAV M-5239.2	-	DoN Cyberspace Information technology and CS Workforce Management and Qualification Manual, June 2016
SECNAVINST 5239.20A	-	Department of the Navy Cyberspace Information Technology and CS Workforce Management and Qualification, 2 May 2016
CNNS Instruction 1253	-	Security Categorization and Control Selection for National Security Systems, October 2009

2.1 Other Publications

American National Standards Institute/American Society of Quality Q9001-2008, Q9000-2005 and Q9004-2009.

FAR 52.204-9 – Personal Identity Verification of Contractor Personnel.

FAR 252.204-7012 – Disclosure Of Information.

NAVEDTRA 130 Series Documents – NETC training content and management guidance documents.

NETC Course Development, Revision, and Modification End-to-End (E2E) Process Standard Operating Procedures (SOP).

NETCINST 1500.9 – Training Requirement Identification and Resource Sponsor Commitment.

NETCINST 1510.3 – Business Case Analysis Policy.

NIST SP 800-171 – Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.

3. REQUIREMENTS

The contractor shall provide AIM software engineering, Instructional Systems Design Analysis, content development and documentation, logistics, and life cycle support services in accordance with (IAW) the requirements set forth in this PWS and the contract.

3.1 General Requirements

3.1.1 Program Management

The contractor shall:

a. Organize, coordinate, and control the program activities to ensure compliance with the contract requirements and the delivery of the required product and services.

b. Provide the personnel, materials, equipment, and facilities to provide the services described in this PWS and all task orders issued under this contract.

c. Provide the program management, systems engineering, design engineering, materials, services, equipment, facilities, testing, technical, logistics, and clerical support for the efforts described in this PWS.

d. Measure, monitor, and assess the progress of the work performed and costs incurred under the contract.

3.1.1.1 Facility(s) Access

The contractor shall allow the government access to the contractor's facility(s) for the purpose of reviewing the contractor's performance on this contract, and allow the government to review internal contractor's documentation pertinent to this contract effort at any time during the period of performance of this contract.

3.1.1.2 Security (Unclassified Systems)

The security requirements specified herein shall apply to the contractor and subcontractors. The contractor shall comply with applicable on-site security regulations related to facility access and building access.

a.

3.1.1.3 Contractor - Owned Unclassified Network Security - Safeguarding of Unclassified Controlled Technical Information

The safeguarding of Controlled Unclassified Technical Information applies to prime contractors and their subcontractors, if applicable, for information resident on or transiting through contractor unclassified information systems. The contractor shall provide security to safeguard unclassified controlled technical information on their unclassified information systems from unauthorized access and disclosure. The contractor shall take means (defense-in-depth measures) necessary to protect the confidentiality, integrity, and availability of Government controlled unclassified information to include the following:

a. The contractor shall manage and maintain contractor-owned unclassified IT network assets used to process U.S. Government controlled unclassified information (sensitive information) IAW FAR 252.204-7012.

1) The security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," http://dx.doi.org/10.6028/NIST.SP.800-171 that is in effect at the time the solicitation is issued or as authorized by the Contracting Officer, as soon as practical, but not later than December 31, 2017. The Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award; or

2) Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection accepted in writing by an authorized representative of the DoD CIO;

b. Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in FAR 252.204-7012, may be required to provide adequate security in a dynamic environment based on an assessed risk or vulnerability.

3.1.1.3.1 Cyber Incident and Compromise Reporting

The contractor shall report to DoD cyber incidents that affect unclassified controlled technical information resident on or transiting contractor unclassified information systems set forth IAW FAR 252.204-7012. The contractor shall report the incident to < at http://dibnet.dod.mil. > and to the COR and NAWCTSD program manager.

3.1.1.3.2 Personnel Security - Background Check (Physical Access to and Working on DoD Installations)

The Common Access Card (CAC) shall be the principal identity credential for supporting interoperable access to DoD installations, facilities, buildings, controlled spaces, and access to U.S. Government information systems IAW FAR 52.204-9. A National Agency Check with Local Agency Checks including Credit Check (NACLC) will be required for permanent issuance of the credential. There shall be no additional NACLC submission for an individual holding a valid national security clearance. The Government may issue the credential upon favorable return of the Federal Bureau of Investigations (FBI) fingerprint check, pending final favorable completion of the NACLC. Access to restricted areas, controlled unclassified information (sensitive information), or Government Information Technology by contractor personnel shall be limited to those individuals who have been determined trustworthy as a result of the favorable completion of a NACLC or who are under the escort of appropriately cleared personnel. Where escorting such persons is not feasible, a NACLC shall be conducted and favorably reviewed by the appropriate DoD component, agency, or activity prior to permitting such access. For contractor personnel performing sensitive duties including access to controlled unclassified information, but not access classified information, the contractor shall use the Standard Form 86 (Questionnaire for National Security Positions) in order to obtain the CAC. The contractor shall submit the Standard Form 86 to the NAWCTSD Security Office for processing.

3.1.1.3.3 Personnel Security – Background Checks

Contractor personnel shall undergo the company internal vetting process prior to gaining access to U.S. Government controlled unclassified information. To comply with immigration law, the contractor shall use the Employment Eligibility Verification Program (E-Verify) IAW FAR 52.222-54. The contractor shall ensure that foreign persons, as defined under section 120.16 of the International Traffic and Arms Regulation (ITAR) (22 CFR, Parts 120 – 130), are not given access to U.S. Government controlled unclassified information, sensitive information, defense articles, defense services, or technical data, as defined in the ITAR, Part 120, without proper issuance of an export license from the U.S. Government authority.

3.1.1.3.4 Personnel Security – Reporting of Adverse or Derogatory Information related to Contractors

The Contractor shall report to the NAWCTSD Security Office adverse or derogatory information pertaining to on-site CSS personnel (when applicable) or contractor personnel in direct support of this contract. Information reported to the Government Contracting Agency shall be integrated and reported in Contractor Performance Assessment Reporting System (CPARS) on contractor

performance of PERsonnel SECurity (PERSEC) related aspects of contractor performance. The following information shall be reported to the NAWCTSD Security Office as applicable:

a. Adverse or derogatory information reporting of contractor personnel. Example: Domestic violence arrest or other violent or sexual crime arrest or self-report.

b. When contractor personnel receive a revocation of an Interim or denial for the issuance of a CAC until final adjudication.

c. When a denial or suspension of clearance occurs for a contractor employee.

d. When contractor employee receives a final denial of eligibility for a security clearance.

3.1.1.3.5 Cybersecurity (CS) and Personnel Security Requirements for Accessing Government Information Technology (IT) Systems

The contractor shall comply with the CS and personnel security requirements for accessing U.S. Government IT systems specified in the contract. Contractors requiring access to U.S. Government IT systems will be subject to a background check. The contractor shall review and become familiar with the credentialing standards presented in OPM Memorandum for Issuing Personal Identity Verification cards to use as an aid in their employee selection process. The NAWCTSD Security Office will apply the credentialing standards and execute the credentialing process for individual contractors.

3.1.1.3.6 Contractor "Out-processing" Policy

The contractor and subcontractor(s), when applicable, shall have in place (established and enforced) an "out-processing" policy for employees that leave the company, including suspension of account access, return of all PCs, laptops, smartphones, and other electronic devices (Government-furnished IT equipment and contractor-issued IT equipment) that contain U.S. Government Controlled Unclassified Information. The contractor shall also ensure that out-processed employees receive debriefings on the need to maintain confidentiality of U.S. Government Controlled Unclassified Information.

3.1.1.3.7 Transmission of Controlled Unclassified Information (CUI) by E-mail

Unclassified e-mail containing CUI shall be encrypted. The contractor shall implement DoD compliant Private Key Infrastructure (PKI) certificate that enables electronic transmission via unclassified networks while protecting the CUI with a digital signature and encryption.

3.1.1.3.8 Transmission of Controlled Unclassified Information (CUI)

Safe Access File Exchange (SAFE). SAFE is designed to provide an alternative way to send encrypted files other than email. Information regarding the use of SAFE can be found at https://safe.amrdec.army.mil/safe/Default.aspx. The contractor shall ensure the following:

a. All files transferred via SAFE shall be for official US Government related business.

b. All files transferred via SAFE shall be UNCLASSIFIED.

c. SAFE CANNOT be used to transmit classified information.

d. All files shall be encrypted.

3.1.1.3.9 Information Security Requirements for Protection of Unclassified DoD Information on Non-DoD Systems

The contractor shall safeguard unclassified DoD information stored on non-DoD information systems to prevent the loss, misuse, and unauthorized access to or modification of this information. The contractor shall:

a. Refrain from processing DoD information on public computers (e.g., those available for use by the general public in kiosks or hotel business centers) or computers that do not have access control.

b. Protect information by no less than one physical or electronic barrier (e.g., locked container or room, login and password) when not under direct individual control.

c. Sanitize media (e.g., overwrite) before external release or disposal.

d. Encrypt the information that has been identified as Controlled Unclassified Information (CUI) when it is stored on mobile computing devices such as laptops and personal digital assistants, or removable storage media such as thumb drives and compact disks, using the best available encryption technology.

e. Limit information transfer to subcontractors or teaming partners with a need to know and a commitment to at least the same level of protection.

f. Transmit e-mail, text messages, and similar communications using technology and processes in accordance with National Institute of Standards Technology Federal Information Processing Standards (NIST FIPS), given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and Transport Layer Security (TLS).

g. When traveling, encrypt organizational wireless connections and use encrypted wireless connections. When encrypted wireless is not available, encrypt application files (e.g., spreadsheet and word processing files), using no less than application-provided password protection level encryption.

h. Transmit voice and fax transmissions only when there is an assurance that access is limited to authorized recipients.

i. Provide protection against computer network intrusions and data exfiltration, including no less than the following:

   1) Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.

   2) Monitoring and control of inbound and outbound network traffic (e.g., at the external boundary, sub-networks, individual hosts) including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.

   3) Prompt application of security-relevant software patches, service packs, and hot fixes.

j. Comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., Critical Program Information (CPI), Personally Identifiable Information (PII), and export controlled information).

3.1.1.4 Management Planning

The Contractor's Configuration Control and Quality Assurance Process plans shall be clearly detailed in the management plan. The contractor shall include a risk mitigation plan that details identification, classification, planning, tracking, and resolution of risk in the management plan. The contractor shall also identify their single point of contact (POC) for the contractual effort.

3.1.2 Software File Transfer Capability

The contractor shall possess and employ the capability to perform electronic bi-directional transfer of government compatible computer files and other pertinent data and program information to the AIM SSO.

3.1.3 Navy-Marine Corps Intranet (NMCI) and Information Assurance (IA) Compliance

The contractor shall meet NMCI certification requirements for AIM software developed that is hosted by NMCI or run on NMCI workstations. The contractor shall comply with NMCI replacement policy. The contractor shall also test, verify, and document that the software developed is in compliance with the security requirements and applicable Information Assurance controls identified in DODI 8510.01.

3.1.4 Software Product Design

The contractor shall perform the software detailed design activities and tasks as specified in IEEE 12207-2008, section 7.1.4.3 to provide the software documentation and software design that can be verified against the requirements and the software architecture, and is sufficiently detailed to permit coding and testing. The contractor shall prepare and deliver the Software Product Design (SPD) document IAW CDRL (A001).

3.1.5 Post-Award Conference (PAC)

The contractor shall attend a government-scheduled post award conference that shall not exceed two days at the contractor's facility within forty-five days after award in which the contractor's lead management, functional, technical, and contractual personnel are in attendance. The government will prepare the agenda, and the contractor shall prepare and deliver meeting minutes IAW the Conference Minutes IAW CDRL B001.

3.1.5.1 Initialization Phase

The contractor shall implement an initialization plan to familiarize themselves with the AIM software, related source code, the NAVEDTRA 130 Series and MIL-PRF-29612B series documents, and be fully operational to meet the requirements of this PWS thirty (30) days from the first task order award. By the end of the initialization phase, the contractor shall obtain and have in place all required personnel, materials, equipment, and facilities to execute the tasks of this contract.

3.1.6 Facility

All tasks are conducted at the contractor's facility unless otherwise indicated within individual task orders.

3.2 Specific Requirements

3.2.1 Core Software Sustainment

The contractor shall furnish the following core software sustainment services:

3.2.1.1 Logistics Support

The contractor shall provide logistics support to the AIM SSO within five work days as set forth by the government for each task. This support shall consist of the following tasks:

3.2.1.1.1 Program Planning and Life Cycle Model Management

The contractor shall define, document, manage, and apply program planning processes for software implementation, configuration management, and quality assurance IAW IEEE Std 12207-2008, sections 6.1.2.3.4.5, 6.3.1, 7.1.1.3.1, 7.2.2 and 7.2.3. The contractor shall prepare and deliver their management plan IAW CDRL (B002).

3.2.1.1.2 Work Planning and Scheduling

The contractor shall develop, document, manage, and apply an Integrated Master Schedule (IMS) that presents the contractor's and any subcontractor's plans and schedules to meet the requirements of the contract. The contractor shall develop and document a tiered scheduling system showing the program milestones and prerequisite events, conferences, data submittals, and deliveries. The contractor shall construct the IMS per task order to ensure that the program milestones are met and to ensure that deliveries meet the requirements of the contract. The contractor shall perform analyses of the IMS tasks, compare the IMS tasks to the scheduling baseline, report potential or existing problem areas, and recommend corrective actions to eliminate or reduce schedule impact. The contractor shall revise the IMS, where necessary, to reflect contract changes. The contractor shall use the IMS as a day-to-day execution tool and periodically assess progress in meeting program requirements. The contractor shall prepare the Integrated Master Schedule IAW CDRL B003.

3.2.1.1.3 Government and Contractor Coordination

The contractor shall support the AIM SSO utilizing the following communication formats:

a. Phone-conferencing
b. Web meetings
c. Video Teleconferencing (VTC)
d. Local contractor meetings
e. E-mail correspondence
f. Contractor hosted website for dissemination of AIM information

3.2.1.1.4 Conferences and Meetings

The contractor shall attend and/or participate in a maximum amount of two (2) conferences or meetings per month, not to exceed 24 annually. The meeting could be either an AIM FRB

meeting, or another conference or meeting the government designates for attendance by the contractor.

The contractor shall attend and provide AIM functional and technical support for a maximum of two FRB meetings per year, and each FRB meeting will be no more than five (5) days in length. The FRB meetings will be held in the Orlando, FL or Virginia Beach, VA area at a government facility or other facility indicated by the government. The contractor will be given at least fifteen calendar days advance notice of any FRB meeting and ten calendar days for cancellation of FRB meetings.

The other conferences or meetings will occur in Washington, DC, Virginia Beach, VA, Norfolk, VA, Pensacola, FL, San Diego, CA, New Orleans, LA or Orlando, FL and will not exceed two days in duration. The contractor is given at least fifteen calendar days advance notice of any conference or meeting and ten calendar days for cancellation. The contractor shall prepare agendas, and prepare and deliver meeting minutes IAW the Conference Minutes CDRL B001.

3.2.1.1.5 Weekly and Monthly Status Reports

The contractor shall provide weekly progress and status reports of the current efforts under this contract via telephone. The report shall also identify and contain summary-level information on all on-going task orders, to include status of work completed under each task order and areas of risks. The phone call shall not exceed sixty minutes. The contractor shall prepare and deliver meeting minutes for the weekly meetings IAW the Conference Minutes CDRL B001. The contractor shall provide a summarized monthly progress and status report of the current efforts under this contract IAW the Contractor's Progress, Status, and Management Report/Monthly Status Report CDRL B004.

3.2.1.2 Software Training Sessions

The contractor shall conduct two (2) monthly AIM user training session(s) of the current Navy AIM I, AIM II and the CPM/LO Module User Training Course Curriculum in San Diego, CA and Virginia Beach, VA. The sessions shall not run concurrently unless concurrent sessions can be arranged and agreed upon by both the contractor and the government. The training session shall be a maximum of forty hours in length and be completed within five (5) days with classrooms and supporting infrastructure provided by government after coordination with the hosting facility and contractor. The class shall consist of no more than 25 students. No class will be executed with fewer than eight students without prior approval of the NETC AIM Program Manager. In the event of software modification or other system configuration change, the contractor shall modify the courses in order to accommodate the applicable changes necessary to achieve the intended training objectives.

The contractor is responsible for administration of the training including:

a. Informational website addressing class schedules and locations

b. Quota control

c. Class reservations and reminders

d. Forwarding specific access forms required for classroom computer access to prospective students

e. Entering class scheduling quota information into Corporate Enterprise Training Activity Resource System

At the completion of each training session, the contractor shall require that each student/trainee complete an online course assessment (link will be provided as Government-Furnished Information upon award of this contract). The government reserves the right to cancel and reschedule any of these training sessions ten (10) calendar days prior to session start date at no cost to the government. A short contractor-prepared summary of the training session shall be delivered to the government IAW CDRL A002.

3.2.1.2.1 Software Training Sessions Instructors

The contractor shall utilize qualified instructors who:

a. Are subject matter experts in curriculum development and maintenance

b. Are subject matter experts in the use of AIM to support curriculum development and maintenance activities

c. Have general MS Windows and networking knowledge and experience

3.2.1.3 Software Demonstrations and Design Meetings

The contractor shall support the demonstration/tutorials of software or software design documents to users, potential user communities and stakeholders as requested or approved by the government. These demonstrations shall include design meetings and presentations to NETC stakeholders of functional design documents or preliminary software in development. The demonstrations and design meetings are conducted via web meeting/conference phone and will last no longer than two hours in duration. A maximum of six software demonstrations shall occur per month, not to exceed 72 demonstrations annually.

3.2.1.4 Software Technical Assessments and SW Baseline Deliveries

The contractor shall complete a software quality assessment annually of all delivered source code using Static Code Analysis (SCA) tools designed to ensure that software follows best coding practices. The contractor shall deliver a report summarizing the SW quality assessment results IAW CDRL A003, a copy of the source and executable code, and change pages to the SPD, IAW CDRL A001 as applicable.

3.2.1.5 Software Functional Requirements Matrix (FRM)/AIM Change Request (ACR) Maintenance

The contractor shall maintain the AIM software FRM and ACR matrix IAW the Revisions to Existing Government Documents FRM/ACR Maintenance IAW CDRL A004. AIM FRM and ACR elements are captured by the government and passed to the contractor for inclusion in the FRM and ACR matrix. FRM and ACR elements captured by the contractor (either from AIM users or generated by the contractor) are validated by the government before being added to and maintained in the matrix.

3.2.1.6 Software Trouble Support

The contractor shall provide software trouble support to the AIM SSO. This support shall consist of technical assistance (TA) and response to technical questions concerning the AIM software (including AIM database, vendor software, centralized AIM servers, and other software). No more than four hours of assistance shall be provided per working day. The TRs

are communicated telephonically and/or electronically via email from the AIM SSO or the government provided trouble call tracking system. The contractor shall review, analyze, assess, and resolve each TR using one of those three communication modes. The results of the contractor's analysis of the problem(s) or resolution(s) shall be communicated to the AIM SSO electronically via email and as part of the monthly status report IAW CDRL B004.

3.2.1.6.1 Software Documentation

The contractor shall also prepare short video demonstrations using Captivate or similar software and post on the contractor hosted website describing and demonstrating the applicable software changes. The contractor shall apply the Quality Assurance (QA) process identified in their management plan to each document before it is submitted to the government. The contractor shall prepare and deliver change pages to the Software FRM/ACR Maintenance and the User's Manual as applicable to reflect any software corrective action/modification/enhancement directives IAW CDRLs A004 and A005.

3.2.1.7 Software Modification Rough Order of Magnitude Estimates

The contractor shall provide rough order of magnitude (ROM) estimates for proposed software modifications resulting from change request actions/modification/enhancement directives. There shall be no more than 120 ROMs per year in response to specific FRM & ACR requested by the government. The ROM estimates for each modification shall consist of:

a. A description of the modification and the associated capabilities improvements.

b. Estimated cost (labor hours, travel, etc.) and time required to complete the software modification and testing.

The ROMs shall be documented and provided to the AIM SSO via the weekly meeting minutes and IAW CDRL B001.

3.2.1.8 Transition Support

The contractor shall provide technical support services for a smooth project transition to the successor contractor. The technical support shall contribute to the successor's understanding of the underlying code structure and coding languages utilized in development and maintenance of the AIM software. The contractor shall provide this support one time only during the final month of the contract.

3.2.2 Software Modifications and Product Generation

The contractor shall perform the following tasks related to software modifications.

3.2.2.1 Software Modifications Status Report

The contractor shall adhere to the direction found in the sub-paragraphs for executing AIM software modifications. These modifications, when bundled together, add new software functionality or enhancement, generally resulting in new releases of the AIM software. All software modifications/enhancements are performed and ISD-related products generated IAW the software processes and standards, configuration control, and QA requirements identified in this PWS and in the Contractor's Management Plan. The statuses of these modifications shall be reported in the Contractor's Progress, Status, and Management Report/Monthly Status Report CDRL B004.

3.2.2.1.1 Government-issued Software Modification/Enhancement Directives

The contractor shall modify/enhance and integrate AIM software IAW Government-issued Software Modification/Enhancement Directives based on Software Change Impact Statements that have been selected for implementation. Government-issued Software Modification/Enhancement Directives lead to software releases of new AIM versions. The software releases will support the Ready Relevant Learning initiative with its focus on delivering training in a modular construct through immersive and interactive learning capabilities, providing just in time training for all sailors. The contractor shall ensure that all parts of the AIM system are completely compatible and usable with all changes.

3.2.2.1.2 Test, Verification and Validation of Pre-released Software

The contractor shall test, verify, and validate software modifications/enhancements prior to delivery of a new software version to the government. Test, verification, and validation of the modified/enhanced software shall be performed IAW IEEE 12207-2008, section 7.2.4.3.2 and 7.2.5 to ensure that:

a. Software Modification/Enhancement Directives have been successfully integrated
b. The impending new release integrates with the existing software/hardware
c. Each function is adequately specified
d. System requirements are fulfilled
e. Missing, extraneous, and incompatible requirements are identified
f. The functionality of the system is in compliance with the applicable Modification/Enhancement Directive

The contractor shall provide their Test, Verification and Validation Test Results status and their assessment for Government Acceptance Test (GAT) readiness during the weekly meetings. The contractor Test, Verification and Validation Test Results status and their assessment for GAT readiness shall be delivered IAW CDRL B001.

3.2.2.1.3 Initial Delivery, Technical Assistance, and Revision of a New Software Release (Change Package)

After successful contractor testing, verification, and validation of the software corrections and or modifications tasks, the contractor shall deliver the pre-release software (referred to as a change package) to the AIM SSO. The contractor shall provide technical assistance during government testing of the change package, which will occur after initial software delivery. This assistance shall include providing advice and technical assistance on testing and troubleshooting any issues found during testing. After the government completes its testing, the contractor shall revise the Change Package to correct any and all deficiencies found during testing. After the changes have been made, the contractor shall provide a revised Change Package to the SSO for final government testing including detailed notes describing all changes, new features, and impact on the users. The contractor shall deliver the corresponding Software Government Acceptance Test Procedures for use by the government during GAT IAW CDRL A006.

3.2.2.1.4 AIM Software Government Acceptance Test (GAT)Support

Following successful GAT testing by the government-selected AIM software users, the contractor shall develop and deliver a post-GAT Test/Inspection Report IAW CDRL A007. The contractor shall also deliver change page/s updates to the FRM/ACR Maintenance and the User's Manual to reflect the Change Package software changes to be integrated into the AIM SW baseline IAW CDRLs A004 and A005.

3.2.2.1.5 Support for New Software Release into Production

Following successful final testing by the government, the contractor shall support the integration of new software releases into the production environment adhering to all procedures required by the hosting agency.

3.2.3 Software Training Sessions and Technical Assist Visits

The contractor shall perform the following tasks related to software training sessions, technical assist visits, and conference/meeting attendance and support at locations determined by the government.

3.2.3.1 Software Training Sessions (Off-site)

The contractor shall conduct off-site AIM user training sessions of the current Navy AIM I, AIM II, CPM/LO Module User Training Course Curriculum. The contractor shall conduct no more than twenty off-site sessions annually. The sessions shall not run concurrently with regular training sessions unless concurrent sessions are arranged and agreed upon by both the contractor and the government. The training sessions shall be no more than forty (40) hours in length and shall be completed within five days with classrooms and supporting infrastructure provided by the sponsor. All training shall take place within the 48 states (CONUS). Training shall not commence until coordination between the government, the contractor, and the sponsor has taken place. The contractor shall utilize qualified instructors IAW paragraph 3.2.1.2.1 of this PWS. The completion of each training session shall require that each student/trainee complete an online course assessment, (link is provided as Government-Furnished Information upon award of this contract). The government reserves the right to cancel any of the annual off-site training sessions ten business days prior to session execution, at no cost to the government. In the event of a cancellation in fewer than ten days prior to the start of the session, the contractor shall make its best effort to mitigate cost as a result of the cancellation. The contractor shall submit a proposal for the cancelled services to the government to negotiate a settlement for the cancellation of services. The following items shall be documented by the contractor IAW the Technical Report-Study/Services/Training Summary Report CDRL A002. The summary report of each training session shall also be reported IAW the Contractor's Progress, Status, and Management Report/Monthly Status Report CDRL B004.

3.2.3.2 Technical Assist Visits (Off-site)

The contractor shall provide off-site technical assistance support to the SSO and/or other AIM sites. One work day of technical assistance support is considered one unit. The contractor shall not exceed 60 units per year in support of this task. This support shall consist of:

a. Issue resolution

b. Trouble-shooting

c. Installation support

d. Assistance in software hosting site transition/location change

e. Demonstrations of upcoming software releases

f. Other meetings/services to include work on AIM, its hardware and/or software (including contractor software, AIM database, and other software)

All training is expected within the 48 states (CONUS). The contractor shall prepare a visit report IAW the Technical Report-Study/Services/Technical Assist Visit Report CDRL A008 after each visit. The summary of actions for each visit shall also be reported IAW the Contractor's Progress, Status, and Management Report/Monthly Status Report CDRL B004.

3.2.4 AIM Related Analysis

The contractor shall perform the following AIM-related analytical tasks.

3.2.4.1 Software Modification/Engineering Change Proposals.

The contractor shall prepare no more than thirty (30) annual Engineering Change Proposals in response to complex ACRs or FRM elements. These analyses are documented and delivered IAW the Engineering Change Proposal/Software Modification/Enhancement/Impact Analysis CDRL A009.

3.2.4.2 Instructional Systems Design Analysis Policy and Guidance

In order to ensure the alignment of software, policy and training, the contractor shall analyze existing NETC policy, procedures and guidelines for the end-to-end (E2E) process. The contractor shall offer suggestions for modifications, deletions and additions, and rewrite or generate new policy documents to provide guidance and standards for the creation of training materials, covering all phases from Analysis to Evaluation. Delivery of new Policy and Guidance will be in Phases, starting first with a report from the Analysis, Design, and Development drawn from the documentation listed below and a high-level outline of a new Policy and Guidance approach. The second phase will be with initial drafts of each new proposed manual, with the intention of producing no more than five new Naval Education and Training Manuals addressing each phase of the Analyze, Design, Develop, Implement, and Evaluate (ADDIE) model and School House management as the author deems fit based on the approved outline. The third phase will be final copies of each new NAVEDTRA incorporating recommended changes from the draft review. In order to ensure government concurrence with Contractor Policy and Guidance deliverables, the government will require 60 days for review and comment on each of three phrases of deliverables. Content from the following documents shall be reviewed under this effort.

g. NAVEDTRA 136 (series) Integrated Learning Environment Course Development and Life-Cycle Maintenance

h. NAVEDTRA 132 (series) Navy School House Testing Management Manual

i. NAVEDTRA 137 (series) Job Duty Task Analysis Management Manual

j. NAVEDTRA 138 (series) Front End Analysis Management Manual

k. NAVEDTRA 130 (series) Task Based Curriculum Development Manual

l. NAVEDTRA 131 (series) Personal Performance Profile Based Curriculum Development Manual

m. NETCINST 1500.10A CPM and LO Development

n. NETCINST 1510.4 (series) Job Duty Task Analysis Policy

o. NETCINST 1500.6 (series) Front End Analysis

p. NETCINST 1510.3 (series) Business Case Analysis Policy

q. NETCINST 1500.91 (series)

r. NETCINST 1500.19 (series) E2E Instruction

s. NETC Content Development and Life Cycle E2E Process Standard Operating Procedures.

t. Naval Education and Training Command Block Learning Analysis Standard Operating Procedures

Content contained in the "Navy Training Transformation" WIKI https://navy-training-transformation1.wikispaces.com/1++Start+Here+to+Transfer+to+other+Wiki+%28ISD+or+SOP%29

The results of this analysis shall be documented and delivered IAW CDRL A00A.

3.2.4.3 Instructional Systems Design Analysis for Design, Development, and All Current and Emerging Modes of Delivery Technology

The contractor shall perform the following analytic tasks in any combination in accordance with the current NETC guidance applicable to each separate analysis task order:

a. Front-End Analysis (FEA) (NAVEDTRA 138)

b. Job-Task Analysis (JTA) (NAVEDTRA 137)

c. Training Task Analysis (TTA) (NAVEDTRA 137)

d. Training Systems Requirements Analysis (TSRA) (NEC SOP WIKI Website)

e. Training Media Analysis (BAC NETCINST 1510.3)

f. Training Systems Analysis (NETC SOP)

g. Instructor Led Training Course Development and or Re-Design and Maintenance Analysis (NAVEDTRA 130)

h. Interactive Multimedia Instruction (IMI) Design and Development Analysis (NAVEDTRA 136)

i. Job Performance Aids (JPA) Development Analysis (NAVEDTRA 130/131/136)

j. Business Case Analysis (NETCINST 1510.3)

No more than ten (10) analyses shall be conducted per year. These analyses results shall be documented and delivered IAW CDRL A00B. The high-level status of these efforts shall be included in accordance with the Contractor's Progress, Status, and Management Report/Monthly Status Report CDRL B004.

3.2.5 Contract Data Requirement List (CDRL)

CDRLs are specified within each task order. Appendix A and B located at the end of the PWS includes a general description of CDRLs required in support of this PWS. Specific lists of data requirements shall be provided within each task order.

3.2.6 Materials

The contractor shall purchase materials to meet the requirements of individual task orders. The Government may procure materials directly, or may use the material CLIN on the contract. A material funding allocation CLIN will be made available for the contractor to immediately respond to system development, system failures, and system operation requirements needs. The contractor shall provide 3 price estimates for all individual items with a cost in excess of $500.00. Material purchase requests made under the material CLIN shall be approved by the PCO prior to purchase. Any material remaining after completion of the contract, the costs of which has been reimbursed by the Government, will remain Government property and disposition instructions will be sought from the PCO. The following is a not all-inclusive list of materials to be purchased under the material CLIN:

a. Multimedia materials (including laptop computers)
b. Batteries
c. Cable assemblies
d. Charging devices
e. Storage devices
f. Connectors and connector accessories
g. Portable projectors
h. Peripheral devices (mice, surge protectors, alternate input devices).

3.2.6.1 Materials Inventory Log

The contractor is responsible for maintaining inventory logs for material purchased under the material CLIN. The contractor shall include the inventory status as part of the monthly status report IAW CDRL B004. The following items shall be documented as part of the material inventory:

a. Specific function or requirement for which the purchase is being made.
b. Item name as well as model and serial number.
c. Place and date of purchase.
d. Item location/destination.
e. Item custodian or point of contact.

3.2.7 Travel Requirements

The contractor shall travel as required in support of and as identified on individual task orders.

Appendix A

ENGINEERING DATA

Exhibit A

Data Item	Description	Data Item Description (DID)
A001	Software Product Design (SPD)	DI-SESS-82036
A002	Technical Report- Study/Services – Software Training Sessions Summary Report	DI-MISC-80508B
A003	Technical Report- Study/Services - SW Technical Assessment Report	DI-MISC-80508B
A004	Revisions to Existing Government Documents – Software Functional Requirements Matrix (FRM)/AIM Change Request (ACR) Maintenance	DI-ADMN-80925
A005	Revisions to Existing Government Documents – Software Documentation (User's Manual)	DI-ADMN-80925
A006	Revisions to Existing Government Documents – AIM Software Government Acceptance Test Procedures	DI-ADMN-80925
A007	Test/Inspection Report - AIM Test/Inspection Report	DI-NDTI-80809B
A008	Technical Report- Study/Services – Technical Assist Visit Report	DI-MISC-80508B
A009	Engineering Change Proposal- Software Modification/Enhancement Impact Analysis	DI-CMAN-80639D
A00A	Technical Report- Study/Services - Instructional Systems Design Analysis Policy and Guidance	DI-MISC-80508B
A00B	Technical Report – Study/Services- Instructional System Design Including Analysis For Design, Dev., and All Current and Emerging Modes Of Delivery Technology	DI-MISC-80508B

Appendix B

ADMINISTRATIVE DATA

Exhibit B

Data Item	Description	Data Item Description (DID)
B001	Conference Minutes	DI-ADMN-81250B
B002	Management Plan	DI-MGMT-80004A
B003	Integrated Program Management Report - Integrated Master Schedule	DI-MGMT-81861A
B004	Contractor's Progress, Status, and Management Report - Monthly Status Report	DI-MGMT-80227

Appendix C

Acronyms

ACAS	Assured Compliance Assessment Solution
ACR	AIM Change Request
AIM	Authoring Instructional Materials
CAC	Common Access Card
CCB	Configuration Control Board
CDRL	Contract Data Requirement List
CIO	Chief Information Officer
CLIN	Contract Line Item Number
COMSEC	Communications Security
CONUS	Continental United States
CPARS	Contractor Performance Assessment Reporting System
CPI	Critical Program Information
CPM	Content Planning Module
CUI	Controlled Unclassified Information
CS	Cybersecurity
CSWF	Cybersecurity Workforce
DoD	Department Of Defense
DoDI	Department Of Defense Instruction
DoN	Department Of The NAvy
E2E	End-to-End
ESC	Executive Steering Committee
FBI	Federal Bureau of Investigations
FEA	Front-End Analysis
FIPS	Federal Information Processing Standards
FRB	Functional Requirements Board
FRM	Functional Requirements Matrix
GAT	Government Acceptance Testing
IA	Information Assurance
IAW	In Accordance With
ILE	Integrated Learning Environment
IMI	Interactive Multimedia Instruction
IMS	Integrated Master Schedule
ISD	Instructional System Design
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
IT	Information Technology
ITAR	International Traffic and Arms Regulation
JPA	Job Performance Aids
JTA	Job-Task Analysis
LO	Learning Object
NACLC	National Agency Check with Local Agency Checks

NAWCTSD	Naval Air Warfare Center Training Systems Division
NETC	Naval Education and Training Command
NISPOM	National Industrial Security Program Operating Manual
NIST	National Institute of Standards Technology
NMCI	Navy-Marine Corps Intranet
NSDD	National Security Decision Directive
OPM	Office Of Personnel Management
OPSEC	Operational Security
PAC	Post Award Conference
PERSEC	Personnel Security
PII	Personally Identifiable Information
PKI	Private Key Infrastructure
POC	Point Of Contact
PPP	Personnel Performance Profile
PWS	Performance Work Statement
QA	Quality Assurance
RMF	Risk Management Framewwork
ROM	Rough Order Of Magnitude
RRL	Ready Relevant Learning
SAFE	Safe Access File Exchange
SCA	Static Code Analysis
SOP	Standard Operating Procedures
SP	Special Publication
SPD	Software Product Design
SSO	System Support Office
TA	Technical assistance
TLS	Transport Layer Security
TO	Task Order
TR	Trouble Report
TSRA	Training Systems Requirements Analysis
TTA	Training Task Analysis
UFOUO	Unclassified For Official Use Only